UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/376,384	08/16/1999	GERSHON BAR-ON	U013169-9	6449

140 7590 12/03/2003

LADAS & PARRY
26 WEST 61ST STREET
NEW YORK, NY 10023

EXAMINER	
SEAL, JAMES	

ART UNIT	PAPER NUMBER
2131	

DATE MAILED: 12/03/2003

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/375,384	COHEN ET AL.	
	Examiner	Art Unit	
	James Seal	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *08 August 1999*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *52-88* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *52-88* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. §§ 119 and 120

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

13)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. § 119(e) (to a provisional application) since a specific reference was included in the first sentence of the specification or in an Application Data Sheet. 37 CFR 1.78.

a) ☐ The translation of the foreign language provisional application has been received.

14)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121 since a specific reference was included in the first sentence of the specification or in an Application Data Sheet. 37 CFR 1.78.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449) Paper No(s) *8-7-8* .
4) ☐ Interview Summary (PTO-413) Paper No(s). _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: .

DETAILED ACTION

1. This Action is in response to applicant's correspondence of 18 August 1999.

2. The IDS's of 9 December 1999, 19 November 1999, 6 March 2000 have been considered and signed copies returned with this Action.

3. Claims 1-51 have been cancelled with prejudice.

4. Claims 52-88 are pending.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

5. Claims 52-63, 66, 68-75, 78-81, 83-84 are rejected under 35 U.S.C. 103(a) as being unpatentable over Moos 5881152 A, and further in view of Anon, IBM TDB NN 85122861.

6. As per claim 52, the limitation of a plurality of intelligent programmable memory chip installed on a data storage medium of data storage devices is disclosed by Moons (Column 2, lines 1-4, and lines 16-17). The data stored on these devices is encrypted with a different encryption key which servers distinguish different systems from one another (Column 2, line 38-39). The chip installed on the data storage medium can communicate with a computer external to the storage medium (Column 2, lines 53-55). Moos further discloses that the storage medium to include optical storage devices (or DVD) Column 2, lines 17-20. Moos is silent on the use of a first antenna connected to

the chip on the optical storage device and a second antenna connected to the optical storage device reader (player). Nor does Moos disclose making the player chip detachable from the player its. Anon teaches combining a storage medium layer, with a layer of integrated electronic circuits using a semiconductor substrate and standard semiconductor fabrication techniques, such that the integrated circuit has memory, logic function, input/output and is able to carry out computations and thus functions as a processor (that is an embedded "chip"). The electronics on the rotating disk are coupled to external circuitry which allows them to exact power, and function as a data input/out port using wireless means, which according to the Anon could include transformer coupling, or capacitive or electro-optical. The diagram (page 2) illustrates wireless connection through two coils on fixed and one attached to the rotating disk. These coils serve as the antennas, one connected to the embedded "chip" the other connected to external circuitry indicated by Anon to be a computer (hence another chip or processor). The "chip" in this case is the semiconductor lay of the disk, is ideally suited for both static and dynamic balancing as the mass of the "chip" is spread throughout the disk. On of ordinary skill in the art at the time of the invention was made, would have motivated to modify Moos with Anon, because Anon's distributed chip would allow a lot more memory and logic gates (such a system could employ FPGA technology) to be incorporated and thus increase the computation resources and power of the "smart disk". Further such a disk is very tamper resistance and hard to reverse engineer, thus increasing the security over the system proposed by Moos. The limitation to make the chip in the player detachable (separable) would also be obvious

to one of ordinary skill in the art at the time that the invention were made because it would allow upgrades. Claim 52 is rejected.

7. As per claim 53, the limitation of common content for two disk is disclosed by Moos Column 3, lines 31-33. Moos teaches the use of his invention for copy prevention (and hence copy protection) for digital content on his disk. Thus Moos teaches more than one disk having the same content as there is no need for copy protection if a single copy of the digital content suffices. Claim 53 is rejected.

8. As per claim 54, the limitation that the security key for audio and video content is different. Video and the correspond audio are general separately because of bandwidth differences and processing differences. Thus one of ordinary skill in the art at the time the invention was made would have been motivated to store these two digital contents separately (even through they are connected with the same creative work) because of the different file format and processing requirements. Further encryption under a different key would provide more security to the creative work. Claim 54 is rejected.

9. As per claim 55, the limitation that the DVD disk is statically balanced was addressed with claim 52. As the "chip" in the Anon teaching has a disk configuration, it is already "substantially" statically balanced. Claim 55 is rejected.

10. As per claim 56, the limitation that the that the DVD disk is dynamically balanced wass addressed with claim 52. As the "chip" in the Anon teaching has a disk configuration, it is already "substantially" dynamically balanced. Claim 56 is rejected.

11. As per claim 57, the limitation that the player security chip decrypts data received from said disk "chip" . According to the teaching of Moos, the data is encrypted with

the secret key stored in the memory are of the disk "chip" (Column 2, lines 64-66). The data is decoded (decrypted) by the target system (the external computer Column 3, lines 6-14) using the security software of the target system (Column 3, lines 3-5) and hence is decrypted by the reader (or player) security chip. Claim 57 is rejected.

12. As per claim 58, the limitation that the "player" chip is integrated into a circuit of an integrated receiver decoder is disclosed by Moos (Column 3, lines 10-12, line 17). Moos teaches the use of the same compression algorithm for reading the data from the disk as writing the data to the disk, and in line 17, Moos teaches decoding the compressed data. If it is not already inherent that the decoder is in the read/right unit of the disk storage reader (player), then one of ordinary skill in the art at the time of the invention would have strong motivation to place it there because the read/write functions are tied up with encoding and decoding. Claim 58 is rejected.

13. As per claims 59-60, the limitation that the player security chip is generally tamper-resistance by Moos (Column 1, lines 6-8). Moos teaches preventing or identifying tampering of stored data (Column 1, line 7), but is silent on the specifics, however, recognizing that the chip within the player is very susceptible to tampering as generally the board on which is mounted chip is mounted if freely accessible to attackers who wish to disable the copy protection or remove it entirely. Further, preventing the cloning of chips would be a specific case of tampering resistance as the chip must be read or reverse engineered to permit cloning. Thus one of ordinary skill in the art at the time the invention was make would have been motivated to apply the

standard methods of tampering heeding the warning of Moos to implement tamper protection to the security chip in the player. Claims 59-60 are rejected.

14. As per claims 61-62, the limitation that the player chip should be upgradeable or backward compatible. Moos is silent on whether his system is upgradeable or backward compatible however one of ordinary skill in the art at the time the invention was made would have been motivated to have incorporated the capabilities of upgrading and making compatible changes to the system because as the system itself is upgrade due to changes in standards (e.g. MPEG) one would need to have these capabilities as a selling point for the system. Claims 61 and 62 rejected.

15. As per claim 63, the limitation that the player security chip performs authentication with the disk security chip is disclosed by Moos Column 2, lines29-32 lines 43-45. Claim 63 is rejected.

16. As per claim 66, the limitation disk security chip performs an authentication process with the player security chip. Moos disclose such authentication Column 2, line 43-45; Column 3, lines 1-3 and figure 2 units 20 and 30 constitute the player). Claim 66 rejected.

17. The limitation of claims 68-75, parallel the claims 52 and 57-63 in which the content of the storage medium is not restricted to audio, video or software. Thus the Moos/Anon would satisfy this broader limitations. Claims 68-75 are rejected.

18. Claim 78 is a method claim corresponding to device claim 52, with the added limitation that the disk key is not known to a disk manufacturer. Moos/Anon is silent with regards to who should known the keys, however, one of ordinary skill in the art

would have no motivation to give the key to the disk vendor because they are not involved in the encryption of the disk content. Claim 78 is rejected.

19. Claim 79 is a method claim corresponding to device claim 52, with the added limitation providing player keys during a predetermined time. Moos/Anon combination is silent on providing player keys during a predetermined time, however, one of ordinary skill in the art would have been motivated at the time the invention was made to have provided such a policy because providing upgrades would necessitate distribution within a well defined time frame to promote user good will. Claim 79 is rejected.

20. As per claim 80, the limitation of encrypting the content of the disk with the disk key. Moos teaches encryption of the disk content in data storage area of the disk using keys stored in the embedded chip (Column 1, lines 41-42; 53-55). Claim 80 is rejected.

21. As per claim 81, the limitation of performing authentication between the player security chip and the disk security chip is disclosed by Moos Column 2, lines29-32 lines 43-45. Claim 81 is rejected.

22. As per claim 83, the limitation that after the disk security chip has verifying that the player is authentic, sends the player the disk key. Moos teaches validating the player (Figure 2 elements 20/30) Column 3, lines 7-12 (here authentication is through the symmetric key and challenge response), the disk chip sends a key that permits decoding (decryption). Claim 83 is rejected.

23. As per claim 84, the limitation that the disk chip sends the player the disk key encrypted by the player key is disclosed by Moos. Moos teaches that the chip contains the public key pair and the symmetric key (Column 2, lines 29-32). Further Moos

teaches that the *private* key of the public key pair is used to *encrypt* the digital data content stored on the disk (Column 2, lines 64-66), and hence the private key is the content key. The secret key of the symmetric key system is used for mutual authentication between the player and the disk chip (Column 3, lines 7-12) and in particular would be the player key as all user must have it in order to perform the authentication (Column 3, lines 3-5). The *public* key of the public key pair is then read from the disk chip and used to *decrypt* (decode) the content. It is inherent in this system that the public key must be kept secret and this is the reason why it is stored on the disk chip. It is inherent because if the public key were truly public then it could be used to by-pass the copy protection of the system. Thus it must be sent to the player to perform the decryption using the security software. But if it in sent in the open, again the system would be compromised, and hence it must be encrypted. Again the only key available to both parties is the symmetric key (player key) and hence the chip encrypts the public key using the player key and sends it to the player. Claim 84 is rejected.

24. As per claim 64, the play security chip verifies legitimacy of disk security chip by means of a function of a geometric property of the DVD. Litman teaches the use of geometry to authenticate and in particular items such as credit cards, smart cards, compact disks (Column 1, lines 30; Column 2, line 11)and further devices used in reading them such as compact disk player, CD-ROM drives, Floppy, optical or floptical disk drives (Column 1, lines 33-39). One of ordinary skill in the art at the time that the invention was made would have been motivated to modify the Moos /Anon system provides a simple solution to piracy and counterfeiting (Column 2, lines 13-21 Litman).

According to Litman, piracy and counterfeiting is costing the economy billions of dollars. Claim 64 is rejected.

25. As per claim 65, Moos and Anon are silent on the limitation that the geometric function depends on angle, diameter, thickness and eccentricity of the DVD. Litman teaches the use of geometric functions such as angle (Column 17, lines 32-34), dimensions of object (length, width, thickness, diameter) Column 7, lines 31-51, Litman, and finally eccentricity (which is defined in terms of terms of the major and minor diameters of an elliptical object and hence a function of dimensions). It would have been obvious for one of ordinary skill in the art at the time the invention was made, to combine the teaching of Moos and Anon with those of Litman because variation of geometry (angles, dimensions, etc.) is hard to copy when copying information onto a new disk. Variation of manufacturing insures this. Note here the angle here involves the layers of the disks rather than artificially introduced elements, but again due to variations in manufacturing techniques, the measurement of these also provides a unique identifier. Claim 65 is rejected.

26. The limitation of claims 76 and 77 are the same as claim 52 and dependent claim 63 combined and in claim 64 the limitation of eccentricity is dropped. Thus the Moos/Anon/Litman combination would also apply. Claims 76-77 are rejected.

27. As per claim 85, Moos and Anon are silent on the limitation of identifying (ID) and validating the disk key using a function of geometry of the disk Litman teaches using geometric feature such as angle, dimensions (including length, width, thickness, diameter, etc.) to identify and validation objects. It would have been obvious for one of

ordinary skill in the art at the time the invention was made, to combine the teaching of Moos and Anon with those of Litman because variation of geometry is hard to copy when copying information onto a new disk. Variation of manufacturing insures this. Further Moos teaches tamper proof storage (Column 1, line 7-8) hence tamper proof storage and variable manufacturing techniques insure that validation of the disk key can be performed in a unique way. Claim 85 is rejected.

28. As per claim 86, the limitation that the geometric property is the angle between layers is disclosed Column 17, lines 33-35. Note here the angle here involves the layers of the disks rather than artificially introduced elements, but again due to variations in manufacturing techniques, the measurement of these also provides a unique identifier. Claim 86 rejected.

29. As per claim 88, the limitation of a method for securing a DVD with a disk security chip connected to a first antenna disposed in the DVD and a second antenna connected to a player chip in the player (See Moos Column 2, and Anon lines 1-11; 20-23). The player security chip verifying the legitimacy of the disk by means of a function of geometry property of the DVD (Litman, Column 7). Claim 88 rejected.

30. Claims 64-65, 76-77, 85-86, 88 are rejected under 35 U.S.C. 103(a) as being unpatentable over Moos/Anon as applied to claims 52-63 above, and further in view of Litman US 5988500 A.

31. Claims 67, 82 are rejected under 35 U.S.C. 103(a) as being unpatentable over the Moos/Anon/Litman combination as applied to claim 66 above, and further in view of Menzes et. al. Handbook of Applied Cryptography.

32. As per claim 67, the limitation that the authentication process is a zero-knowledge interaction. Menzes teaches Interactive zero-knowledge protocols pages 406-410. One of ordinary skill in the art at the time the invention was made, would have been motivated to modify the Moos/Anon/Litman combination with the interactive zero-knowledge proof because there is no leakage of information in either direction. Claim 67 is rejected.

33. As per claim 82, the limitation that the authentication process consists of mutual zero-knowledge interaction Menzes teaches Interactive zero-knowledge protocols pages 406-410. One of ordinary skill in the art at the time the invention was made, would have been motivated to modify the Moos/Anon combination with the interactive zero-knowledge proof because there is no leakage of information in either direction. Claim 82 is rejected.

34. Claim 87 is rejected under 35 U.S.C. 103(a) as being unpatentable over Moos/Anon combination as applied to claims 52-86 above, and further in view of Clark et. al. A Survey of Authentication Protocol 17 November 1997.

35. As per claim 87, the limitation that the player security chip authenticates the disk security chip by symmetric key is taught by Moos (Column 2, lines 33-34). Moos is silent as to which symmetric key authentication is used. Clark discloses a symmetric key K_{ab} two party protocol using a non-reversible function (a hash function) f and nonce R in section 6 of his paper entitled A Library of Protocols 6.1.5. Using the terminology B for the Player security chip (the first party) and A the disk security chip and R_b = R for

the nonce (random number). The player sends a random number R to the disk. The disk A hashes the random number R as f(R) send the content key K along with the hash encrypted under the symmetric key Kab that is $E_{K_{ab}}$ (f(R) , K) back to the player chip (B). The player B is then free to hash R and compare it to what was sent by the disk chip A. If they match then the player chip B has authenticated the disk chip A (step 3 is not needed as the claimed authentication is not mutual). The content which the viewer is entitled to view may then be decrypted. Claim 87 rejected.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to James Seal whose telephone number is 703 308 4562. The examiner can normally be reached on M-F, 8-5.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gail Hayes can be reached on 703 305 9711. The fax phone number for the organization where this application or proceeding is assigned is 703 746 7239.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is 703 308 3900.

James Seal

James Seal
Examiner AU 2131
25 November 2003